Blog
"Security and the Internet of Things"
MIT Sloan

Stuart Madnick

Working Paper CISL# 2016-20

November 2016

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Blog: Security and the Internet of Things
By Stuart Madnick

Stuart Madnick is the John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management, and Professor of Engineering Systems, MIT School of Engineering and the founding Director of the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, also known as (IC)[3]

My brother can't function in the morning until he has a cup of coffee. So I use his daily routine as an example.

Picture my brother stumbling down to the kitchen one morning only to find his internet-enabled coffee maker won't work. There's a message on his iPhone: "We have taken control of your coffee pot and unless you pay $5, you won't have your coffee." This actually hasn't happened. At least, not yet.

I have been talking about the security threats to common household items connected to the internet – that is, the Internet of Things (IoT) – for several years now, and unfortunately, every other dire warning has come true so far. Upper management has to take greater notice of risks exposed both in the products they produce and the products that they use and take action to mitigate those risks. Recent events underscore this need.

Two years ago an internet-enabled refrigerator was commandeered and began sending pornographic spam while making ice cubes. Baby monitors have been turned into eavesdropping devices and there are concerns about the security of medical devices, such as computerized insulin pumps. In October, thousands of security cameras were hacked to create a massive Distributed Denial of Service (DDoS) against Dyn, a provider of critical Domain Name System (DNS) services to companies like Twitter, AirBnB, etc. These are only a few examples highlighting the threats.

Meanwhile, smart devices continue to proliferate. Gartner, Inc. forecasts that 6.4 billion connected things will be in use worldwide in 2016, up 30 percent from 2015, and will reach 20.8 billion by 2020.

Threats to IoT can be divided into two categories. First, devices are taken over to do something they are not intended to do, like a security camera that becomes part of a botnet attack. But also devices can be commandeered to do exactly what they are intended to do but in a devious way. Think of directing a self-driving car to drive off a bridge. Consider the cyber attack on Iran's nuclear enrichment centrifuges to make them rapidly speed up and then suddenly slow down (imagine pushing down hard on the accelerator, and then the brake in your car), which eventually seriously damaged them. That flummoxed operators who had never planned a response to prevent something like that because why would you do that in the first place?

Therein lies the danger of IoT security flaws: Hackers may come up with ways to use devices that were never conceived of before. Cyber warfare is an evolving risk, but human nature is focused on the way things are supposed to work. This blinds us to the

way things can be made to work. So how do you weigh the risk of something you've never seen before and something you've never thought of? It's a cliché but I compare much of cyber security to people driving their car by looking through the rear view mirror. That is, what will happen next year is likely very different than what happened last year.

What are needed are cultural adjustments by both corporations and consumers. In effect, many consumers are leaving their front doors unlocked and wide open. For example, many home security cameras are operated with just the default password. Remember those blinking clocks you'd see on VCRs when consumers didn't set the time? If people didn't know or bother to set the clock on the VCR are they going to know or bother to change the password on the security camera? Such carelessness has to be modified. By changing passwords and taking other steps, consumers can get a layer of protection. It doesn't mean an attacker can't get through a locked door, but it is just so much easier to get through an open door.

Corporate management must make security a high priority, not something assigned to the junior assistant programmer trainee who, in the old days, went desktop to desktop with the latest Microsoft security patch. It is far too easy for upper management to be oblivious to risks their engineers are putting their company and customers into. But as companies are producing and acquiring more automated products, upper management needs to understand the risks they are creating. The good news is that the understanding is increasing. The bad news is that it is increasing from a low starting point.

A key issue is balancing security with ease of use. Take that blinking clock; like many other device functions, time setting for DVRs has been automated through its connection to the cable or Internet, a benefit to consumers. But automation can open up vulnerabilities and complications. You can make a device more secure but that can make it harder to use. I helped a friend set up a Comcast internet router with its complicated pre-assigned unique 24-character password – it took four tries to get it right. If you're introducing a new device that needs to develop a consumer base, ease of use has to be a prime concern. Benefits and risks must be carefully weighed; while it's cool to speak a command to Google Home or Amazon Echo and get a response, that means such devices are listening ALL the time.

It is great that computer-enabled internet-connect devices now bring wonderful new capabilities and conveniences. But there is also a need to take a broad view of the impact on our nation's critical infrastructure, especially addressing the managerial, organizational and strategic aspects, which is the focus of MIT's Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity.

So far, my brother has been able to get his morning coffee without incident. But what ransom might he pay for a jolt of java on the day that his coffeemaker balks?